Кейс. Расследование атаки: взлом двух компаний через подрядчика

›› Расследование и реагирование

ЖЕРТВА АТАКИ

ИТ-компания, госорганизация, телеком-компания

Цель атаки:
Кража чувствительных данных

Уровень атаки:
Продвинутая

APT-группировка:
NGC 5081

ДЕТАЛИ АТАКИ

Взлом подрядчика [лето 2024], через которого атакованы два его клиента* [осень 2024 — лето 2025]

Доступ в инфраструктуру клиентов через украденные у подрядчика учетные данные

C2-сервером для ВПО в одном из клиентов выступал сервер подрядчика

* По предположению команды Solar 4RAYS

СХЕМА ХРОНОЛОГИИ АТАКИ

Указана на следующем слайде

РЕШЕНИЕ

Расследование и реагирование на инциденты (DFIR)

ХОД РАССЛЕДОВАНИЯ

В результате анализа активности в SIEM команда Solar JSOC обнаружила атаку на компанию А.

Подключили к реагированию на инцидент команду Solar 4RAYS, которая:

[01] Обнаружила компрометацию инфраструктуры компании X (подрядчик компании А)

[02] По итогу реагирования на инцидент в инфраструктуре компании X выявила следы компрометации серверов компании В (второй клиент компании X)

[03] Нашла следы компрометации инфраструктуры компании В: системы, где были размещены аналогичные файлы вредоносного ПО, что и у компаний А и X

[04] Локализовала инцидент и провела работы по предотвращению повторения инцидента. Разработала для заказчика правила по обнаружению атак [доступны в Solar TI Feeds]

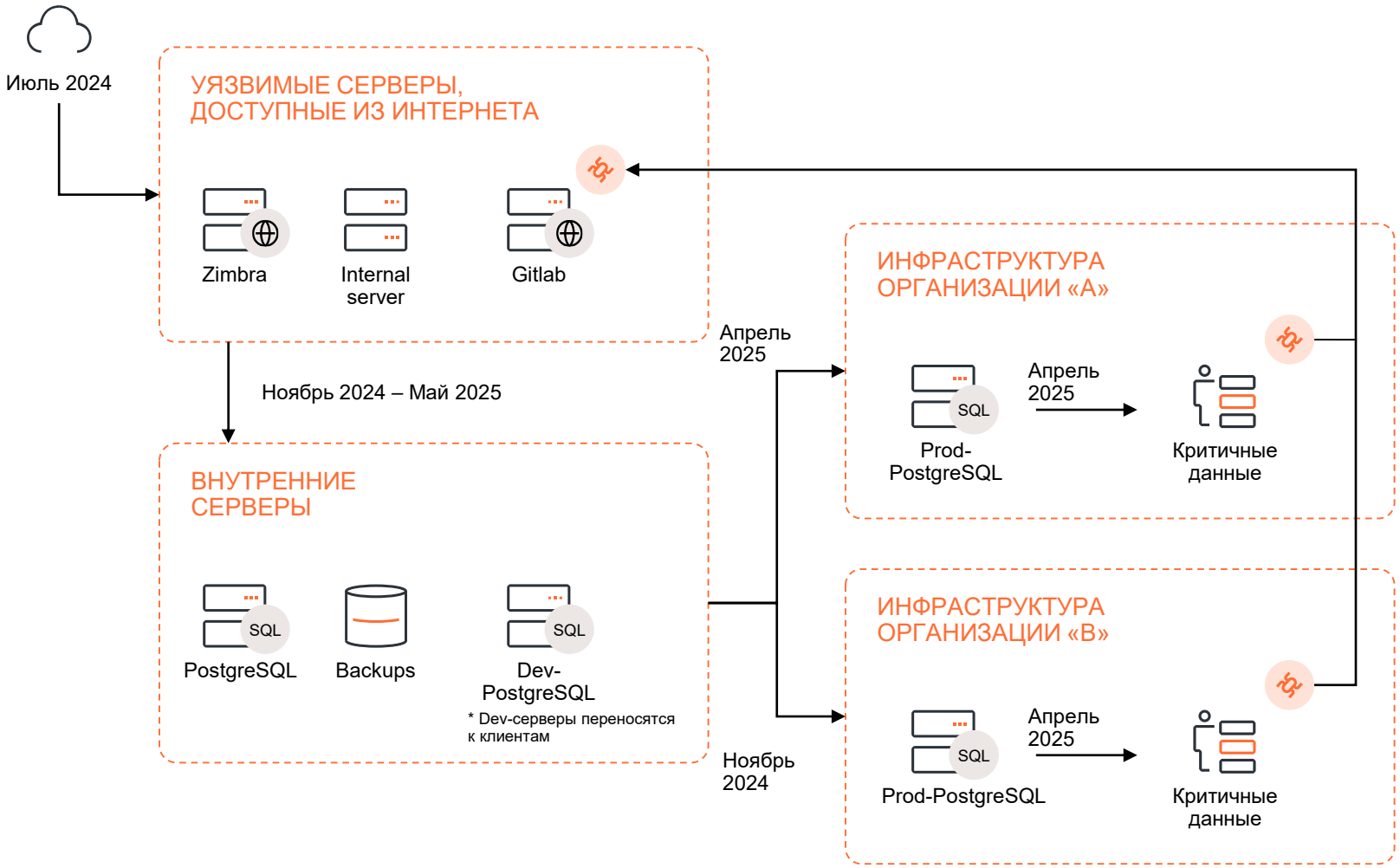
[05] Подготовила отчет с выводами по инциденту и рекомендациями по его недопущению в дальнейшем.

Технические детали расследования доступны в статье блога Solar 4RAYS

Кейс. Расследование атаки: взлом двух компаний через подрядчика

›› Расследование и реагирование

ХРОНОЛОГИЯ АТАКИ



РЕКОМЕНДАЦИИ по возможной остановке атаки и ее предотвращению

- Соблюдение базовых правил кибергигиены Подробнее
- Внедрение системы PAM, контроль доступа подрядчика к инфраструктуре
- Периодическая оценка защищенности инфраструктуры (пентесты, киберучения и т. п.)
- Подключение к мониторингу и анализу инцидентов (SOC)*, потокам данных TI Feeds
- Мониторинг DNS-трафика, блокировка вредоносных и фишинговых доменов
- Проведение Compromise Assessment при подозрении на атаку

** В данном кейсе команда мониторинга Solar JSOC помогла обнаружить атаку и подключить команду Solar 4RAYS к расследованию инцидента*